Sri Sathya Sai College for Women, Bhopal

2017

A newsletter from the Dept. of Computer Sci. & Appl.

CompuTalk Vol. III

- Cyber Security job oppurtunities
- Botnet
- Computer Network
- Firewall
- Departmental News

Department of Computer Science and Application

Now Trending:

Job Opportunities under the Cyber Security Umbrella

Cyber security also known in simpler terms as computer security or IT security involves the protection of computer systems from theft, damage or destruction of their hardware, software, data and information, as well as from disruption, misuse or misdirection of the services provided through them to cause damage to the fellow humans or society.

The role of cyber security involves controlling or limiting physical access to the hardware, as well as protecting them against any harm or attack that may come via network access intrusion, data insertion and code injection and remote control. IT security is susceptible to being tricked into deviating from secure procedures through various methods. This may occur either due to malpractices by operators, which may be either intentional or accidental or in connivance.

The field of cyber security is growing into an utmost important aspect of the world as a whole due to the increasing reliance on computer systems, the Internet, wireless networks such as Bluetooth and Wi-Fi, boom in the development and use of "smart" devices, including smartphones, televisions and tiny devices and integration of these as part of the Internet of Things. Boom in cyber threats has been an integral part of boom in information technology .

Typical cyber security job titles and descriptions may include the following:

1. Security Analyst

A Security Analyst analyzes and assesses vulnerabilities in the infrastructure which includes software, hardware and the associated networks. He/she performs investigation using available tools, suggests counter-measures to remedy the detected vulnerabilities, and recommends solutions and best practices. He/she analyzes and assesses the damage done to the data/infrastructure as a result of security incidents, examines available recovery tools and processes, and recommends solutions. He/she performs tests for compliance with security policies and procedures. His/her role may also include providing assistance in the creation, implementation, or management of security solutions.

2. Security Engineer

A Security Engineer performs security monitoring, security and data/logs analysis and forensic analysis in order to detect security incidents, and mounts the incident response. He/she investigates and utilizes new technologies and processes to enhance security capabilities and implement improvements. He/she may also review code or perform other security engineering methodologies. Security engineering is a specialized field of engineering that focuses on the security aspects in the design of systems that need to be able to deal robustly with possible sources of disruption, ranging from natural

disasters to malicious acts. It is similar to other systems engineering activities in that its primary motivation is to support the delivery of engineering solutions that satisfy pre-defined functional and user requirements, but with the added dimension of preventing misuse and malicious behavior. These constraints and restrictions are often asserted as a security policy.

3. **Security Architect**

A Security Architect designs a security system or major components of a security system, and may head a security design team involved in building a new security system.

4. **Security Administrator**

A Security Administrator installs and manages organization-wide security systems. He/she may also take on some of the tasks of a security analyst in smaller organizations.

5. **Chief Information Security Officer (CISO)**

A Chief Information Security Officer is a high-level management position responsible for the entire information security division/staff. This may include hands-on technical work as regards the security of information is concerned.

6. **Chief Security Officer (CSO)**

A Chief Security Officer is again a high-level management position responsible for the entire security division/staff. This is comparably a newer position now deemed essential as security risks are growing by the day.

7. **Security consultant/Specialist/Intelligence**

Broad titles that encompass any one or all of the other roles or titles are tasked with protecting computers, networks, software, data or information systems against viruses, worms, spyware, malware, intrusion detection, unauthorized access, denial-of-service attacks, and an ever increasing list of attacks by hackers acting as individuals or as part of organized crime or foreign governments.

Student programs are being made available throughout the country on various platforms for individuals interested in beginning a career in cyber security as specialization after graduation. Meanwhile, a flexible and effective option for information security professionals of all experience levels is to keep studying through online courses, trainings and webcasts related to cyber security methodologies.

Abhilasha Kumar:*abhilasha.k00@gmail.com*

Botnets:

The Dangerous Side Effects Of The Internet Of Things

The Internet of Things (IoT) is the name given to describe the relatively new technology that connects everyday objects and devices to the web to provide additional data or functionality. But in the race to create that next “it” product that no one can live without (smart fry pans anyone?), manufacturers and users are creating dangerous side effects known as botnets.

The term botnet simply means a group of internet-connected devices controlled by a central system. But the term is most often used in conjunction with a particular type of malicious hacking, especially Distributed Denial of Service Attacks (DDoS attacks). In this case, a hacker uses a large botnet group of internet-connected devices to flood a website or network resource with fake requests so that legitimate users cannot access it.By using a botnet with hundreds or even thousands of devices, all with

their own unique IP addresses, the hacker makes it almost impossible to stop the attack or distinguish legitimate users from fake ones.

The market has been flooded with inexpensive devices — webcams, baby monitors, thermostats, and yes, even yoga mats and fry pans — that connect to the Internet, each of which has its own IP address. But these devices have little or no built-in security, and even when they do, users often neglect to even take the basic step of setting a password for them. That makes them easy targets for hackers wanting to create and use a botnet.

How botnets work

The term botnet is derived from the words robotand network. A bot in this case is a device infected by malware, which then becomes part of a network, or net, of infected devices controlled by a single attacker or attack group.The botnet malware typically looks for vulnerable devices across the internet, rather than targeting specific individuals, companies or industries.

The objective for creating a botnet is to infect as many connected devices as possible, and to use the computing power and resources of those devices for automated tasks that generally remain hidden to the users of the devices. On its own, that fraction of bandwidth taken from an individual device won't offer much to the cybercriminals running the ad fraud campaign. However, a botnet that combines millions of devices will be able to generate a massive amount of fake traffic for ad fraud, while also avoiding detection by the individuals using the devices.

Botnet architecture

Botnet infections are usually spread through malware, such as a Trojan horse. Botnet malware is typically designed to automatically scan systems and devices for common vulnerabilities that have not been patched, in hopes of infecting as many devices as possible. Botnet malware may also scan for ineffective or outdated security products, such as firewalls or antivirus software.

Notable Botnet attacks

Zeus

The Zeus malware, first detected in 2007, is one of the best-known and widely used malware types in the history of information security.

Srizbi

The Srizbi botnet, which was first discovered in 2007, was, for a time, the largest botnet in the world. Srizbi, also known as the Ron Paul spam botnet, was responsible for a massive amount of email spam -- as much as 60 billion messages a day, accounting for roughly half of all email

spam on the internet at the time. In 2007, the Srizbi botnet was used to send out political spam emails promoting then-U.S. Presidential candidate Ron Paul.

Gameover Zeus

Approximately a year after the original Zeus botnet was disrupted, a new version of the Zeus malware emerged, known as Gameover Zeus. Instead of relying on a traditional, centralized C & amp; C operation to control bots, Gameover Zeus used a peer-to- peer network approach, which initially made the botnet harder for law enforcement and security vendors to pinpoint and disrupt.

Methbot

An extensive cybercrime operation and ad fraud botnet known as Methbot was revealed in 2016 by cyber security services company White Ops. According to security researchers, Methbot was generating between $3 million and $5 million in

fraudulent ad revenue daily last year by producing fraudulent clicks for online ads, as well as fake views of video advertisements.

Mirai

Several powerful, record-setting distributed denial-of- service (DDoS) attacks were observed in late 2016, and they later traced to a new brand of malware known as Mirai. Mirai malware is designed to scan the internet for insecure connected devices.Once it identifies an insecure device, the malware tries to log in with a series of common default passwords used by manufacturers. If those passwords don't work, then Mirai uses brute force attacks to guess the password. Once a device is compromised, it connects to C&C infrastructure and can divert varying amounts of traffic toward a DDoS target.

Preventing Botnet attacks

In the past, botnet attacks were disrupted by focusing on the command-and- control source. Law enforcement agencies and security vendors would trace the bots' communications to whereverthe C&C servers were hosted, and then force the hosting or service provider to shut them down

Protect Against Bots

To safeguard against malicious bots, security experts offer the following advice:

1. Install top-rated security software (such as Norton 360) and Norton AntiBot.

2. Configure your software's settings to update automatically.

3. Increase the security settings on your browser.

4. Limit your user rights when online.

5. Never click on attachments unless you can verify the source.

6. Ensure that your system is patched with the most current Microsoft Windows Update.

7. Set your computer's security settings to update automatically, to ensure you always have the most current system patches.

(Source:https:

//en.wikipedia.org/wiki/BotnetComputer

Babita Sakalle:*babita.sakalle@gmail.com*

Computer Network

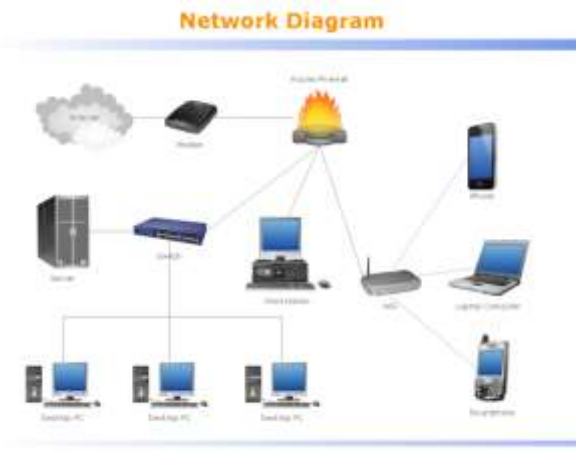
A network is defined as a group of two or more computer systems linked together.

Wired and Wireless Technologies:

Networks may use a mix of wired and wireless technologies. Network devices communicate through a wired or wireless transmission medium.

- Wired networks: This may consist of optical fiber, coaxial cable or copper wires in the form of a twisted pair.
- Wireless network: This includes computer networks that use wireless data connections for connecting endpoints. These endpoints include broadcast radio, cellular radio, microwave and satellite.

Types of Computer Networks:



- Local-area networks (LANs): The computers are geographically close together (that is, in the same building).

- Wide-area networks (WANs): The computers are farther apart and are connected by telephone lines or radio waves.

- Campus-area networks (CANs): The computers are within a limited geographic area, such as a campus or military base.

- Metropolitan-area networks MANs): A data network designed for a town or city.

- Home-area networks (HANs): A network contained within a user's home that connects a person's digital devices.

Network Characteristics:

In addition to these types, the following characteristics are also used to categorize different types of networks:

- Topology : The geometric arrangement of a computer system. Network topologies represent the physical or logical structure of a network. with common topologies that include the following major types:

    - Mesh Network: In this type all nodes are connected to each other and can exchange data.
    - A Tree Network, which is a combination of two or more star networks connected together.
    - A Star Network, in which the nodes are connected to a common central computer.
    - A Bus, a circuit arrangement where all network devices are attached directly to a transmission line directly, and while all signals pass through all devices, each device has a unique identity and recognizes signals intended for it.
- **Protocol** : The protocol defines a common set of rules and signals that computers on the network use to communicate. One of the most popular protocols for LANs is called *Ethernet*. Another popular LAN protocol for PCs is the *IBM token-ring network* .

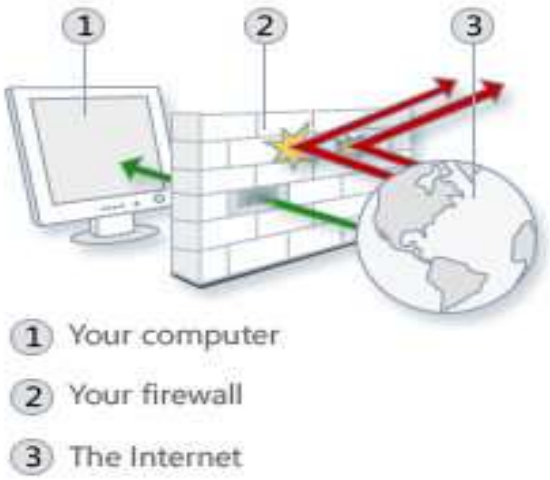
Aruna Sengar:*Sengar.aruna1@gmail.com*

Firewall (Computing)

What is a firewall? A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. If you can't start Windows Firewall or you are getting an error, use our free tool to diagnose and fix problems.

In computing, a firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.[1] A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed to not be secure or trusted.

Originally, a *firewall* was a wall that was built to stop (or slow down) the spread of a fire. In terms of computer security, a firewall is a piece of software. This software monitors the network traffic. A firewall has a set of rules which are applied to each packet. The rules decide if a packet can pass, or whether it is discarded. Usually a firewall is placed between a network that is trusted, and one that is less trusted. When a large network needs to be protected, the firewall software often runs on a dedicated hardware, which does nothing else.



Different kinds of Firewalls

Packet filtering

Data travels on the internet in small pieces; these are called packets. Each packet has certain metadata attached, like where it is coming from, and where it should be sent to. The easiest thing to do is to look at the metadata. Based on rules, certain packets are then dropped or rejected. All firewalls can do this.it is known as network layer

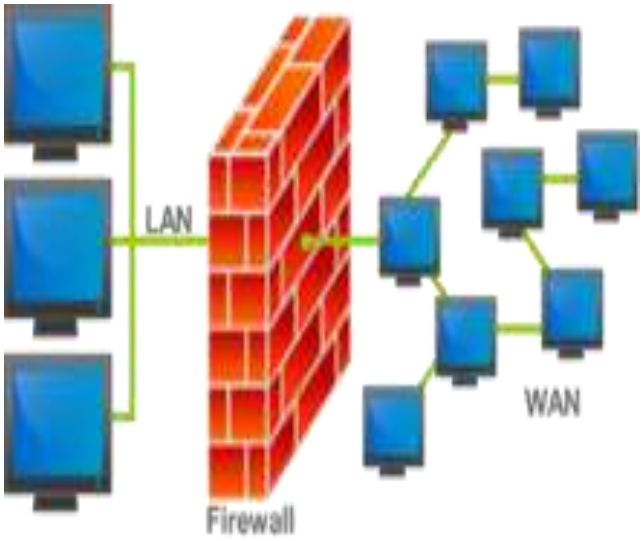
Packet inspection

In addition to the simple packet filtering (above) this kind of firewall also keeps track of connections. A packet can be the start of a new connection, or it can be part of an existing connection. If it is neither of the two, it is probably useless and can be dropped.

Application-layer firewalls

Application-layer firewalls do not just look at the metadata; they also look at the actual data transported. They know how certain protocols work, for example FTP or HTTP. They can then look if the data that is in the packet is valid (for that protocol). If it is not, it can be dropped.

A firewall protects one part of the network against unauthorized access.



Arpana Sinhal:*sinhal.arpana@gmail.com*

Departmental News

Activity/Achievement Report 2017-18

- Asha Gaekwad, Lab. Tech., participated in M.P. State Powerlifting(equipped category) on 7-9th July 2017 and won Silver Medal .She acted as Referee for the competition and was honored for the same .

- Workshop on " Resume Writing " was held on 28th August 2017, in coordination with expert from Appin Technologies, Bhopal , for the final year students.

- A 2- hour seminar and presentation session was organized for the students of Bio Science stream in coordination with ITSC Startup School, Bhopal on the topic " Role of IT in Health Services and Hospital Management" as Career Guidance activity on 4th September 2017.Speakers for the seminar were Mr. Sanjeev Kumar and Ms Neha.

- UGC sponsored 2- day (8 / 11 Sept.) training workshop was organized for Final year students on " Resume Writing and Interview Preparation ", under the career guidance scheme, with expert from the industry, Mrs. Manisha Anand.

- A 6-day UGC sponsored workshop on " PHP & MySQL" under the career guidance scheme was held in the college for commerce students from 18th – 23rd September 2017.

- Campus placement drive was held by CapGemini at LNCT on 14th Sept 2017 for the students of science and computer streams. Two students were selected -

i) Sakshi Mishra B.Sc. V Sem (CS) ii) Pragati Tiwari BCA V Sem.

- A 6-day UGC sponsored workshop on "Financial Accounting & Tax Analysis" under the career guidance scheme was held in the college for BCA and M.Sc. CS students 18th – 23rd September 2017.

- A lecture was organized on 22nd September 2017 ,in coordination with Pune Institute of Business Management, on "Goal Setting and Employability Skills". Expert speaker was Mr. Shashwat Sidhhant, passout of IIM , Ahemdabad.Seminar on " Job opportunity in Airlines Industry" was held for the students of science, and commerce and computer appl. students in coordination with "Fledge Institute of Aviation and Hospitality, Bhopal. Speaker was Mrs. Barnali Singh, Center Head .

- Workshops were organised under the e-shakti abhiyan , to educate students and staff about digital payment procedures and cashless transactions on 18th and 19th September 2017.

- Asha Gaikwad, Lab. Tech., participated in Senior Woman Division Power Lifting Championship held at Nasrullaganj on 7-8th October 2017 and bagged three prizes. I place in "Bhopal-Narmadapuram Division Powerlifting Championship" in 72Kg weight category, "Strongest Woman" and "Best Lifter Woman".

- Workshop on " Advanced features of MS-Excel" was organized in the department for students of computer faculty in coordination with experts from ITDP ,Bhopal on 10th Oct.2017 .

- Students of final year attended open campus drive at Career College on 3rd November 2017, held for placement in Research Panel and Investment Advisors, Indore. Five students of BCA faculty were selected :

    1. Priyanka Singh
    2. Manisha Vishwakarma
    3. Chanchal Sawale
    4. Manjeeta Singh
    5. Disksha Chhapre

- Students of BCA and BSc. Computer Sc. final year registered for the TCS- Open Ignite program to appear for online qualifying exam in the month of December for recruitment to TCS. TCS Open Ignite is specifically designed to prepare them for an IT career and to increase employability. Over all 7 students registered for the test and all have qualified for direct interview:

    1. Priyanka Singh
    2. Pragati Tiwari
    3. Kalpana Parihar
    4. Vandana Verma
    5. Geetanjali Bhondwe
    6. Neha Kumari
    7. Manisha Vishwakarma

- Out of these students Ku. Pragati Tiwari has also qualified for the Software Engineering Industrial Certification from TCS. Interview results are pending as on date.


Computer Lab for UG Students


Computer Lab for UG Classes

Workshop by staff at NSS Camp